POSITIVE TECHNOLOGIES

92% компаний беззащитны перед злоумышленником, атакующим из интернета

50% позволяют злоумышленнику попасть в свою сеть за 1 шаг

В 90% случаев компрометация всей инфраструктуры компании занимает менее 24 часов

197 дней – среднее время присутствия злоумышленника в системе до обнаружения

Каждый третий сотрудник рискует запустить вредоносный код на своем рабочем компьютере

Каждый седьмой сотрудник вступает в диалог со злоумышленником и выдает конфиденциальную информацию

Готов ли ваш бизнес противостоять современным киберугрозам?

Консалтинг и сервисы

Непрерывное повышение защищенности бизнеса от киберугроз

Эмуляция APT-атаки
Поможет оценить и повысить устойчивость вашего бизнеса перед реальной кибератакой

Pentest 365
Обеспечит непрерывное выявление актуальных векторов кибератак на вашу компанию

PT RvB (Red Team vs Blue Team)
Поможет в обнаружении угроз и совершенствовании стратегии реагирования на них

Сегодня практически все бизнес-процессы опираются на цифровые технологии, так или иначе уязвимые к кибератакам. Целью злоумышленника может быть как изменение логики бизнес-процесса, так и полная его остановка — нарушение деятельности компании-жертвы. Как показывает практика, IT-, ИБ-службы зачастую не в состоянии эффективно использовать результаты классического тестирования на проникновение, оставляя для злоумышленников огромную поверхность атаки. Кроме того, злоумышленники давно уже не действуют в одиночку — это целые преступные APT-группировки. Защититься от подобных источников угроз самостоятельно практически невозможно.

Набор уникальных услуг Positive Technologies по повышению защищенности бизнеса от киберугроз поможет вести непрерывную оценку уязвимости именно вашей компании перед действиями реальных злоумышленников и оперативно принимать меры по предотвращению кибератак и устранению их негативных последствий.

Сочетание сервисов моделирования сложных атак и услуг по выявлению угроз позволяет наиболее эффективно выстроить процессы обеспечения защиты ваших бизнес-процессов и минимизировать возможный финансовый и репутационный ущерб от кибератак.

Мониторинг и реагирование на инциденты

Advanced Border Control
Поможет непрерывно выявлять проблемы, возникающие на сетевом периметре компании

Поиск следов компрометации
Выявит следы подготовки к хакерской атаке и признаки компрометации

Реагирование на инциденты и расследование
Поможет оперативно локализовать угрозу и быстро восстановить нормальную работу бизнеса

Positive Technologies Expert Security Center (PT ESC) — экспертное подразделение Positive Technologies. PT ESC предоставляет услуги по реагированию и расследованию инцидентов, а также мониторингу защищенности корпоративных систем на базе продуктов Positive Technologies.

Более 15 лет опыта в анализе защищенности, расследовании деятельности крупнейших преступных APT-группировок и инцидентов, а также мониторинга безопасности крупных компаний позволили нашим экспертам выработать уникальные методы и подходы к практической безопасности.

Услуги PT ESC по непрерывному мониторингу сетевого периметра, ретроспективному анализу результатов работы MaxPatrol SIEM и PT NAD, а также выявлению следов компрометации позволяют оценить реальное состояние защищенности вашей инфраструктуры и выявить развивающуюся кибератаку. Комплекс этих мер позволяет вовремя приступить к устранению найденных проблем, остановить проникновение злоумышленника и предотвратить ущерб бизнесу и репутации компании.

Реагирование и расследование инцидентов — одно из профильных направлений PT ESC. Соответствующие услуги призваны в первую очередь помочь заказчику оперативно определить источник угрозы, локализовать все следы присутствия злоумышленника в системах компании и восстановить нарушенный кибератакой бизнес-процесс.

Отраслевая экспертиза

Блокчейн
Анализ защищенности блокчейн-систем

Банки
Поможет оценить риски и повысить безопасность специализированной инфраструктуры

- Анализ защищенности ДБО
- Анализ защищенности АТМ
- Анализ защищенности POS-терминалов

Промышленность
Поможет оценить риски и принять защитные меры в соответствии с ФЗ-187, приказами ФСТЭК №31 и 239

Отраслевая специфика может накладывать сильный отпечаток на подходы к обеспечению ИБ. Эксперты Positive Technologies накопили богатый опыт работы с финансовыми учреждениями и предприятиями промышленности.

Сегодня блокчейн-технологии (например, на базе Hyperledger Fabric или Ethereum) становятся все более популярными в организациях, в том числе в государственных и финансовых. Атаки на корпоративные блокчейн-системы могут привести к серьезному ущербу. Эксперты Positive Technologies предоставляют необходимый спектр услуг по анализу защищенности блокчейн-систем, исходных кодов смарт-контрактов, а также обучение безопасной разработке смарт-контрактов.

Кибератаки, связанные с выводом денег из банкоматов, получением несанкционированного доступа к системам дистанционного обслуживания клиентов из года в год приносят миллионный ущерб банкам и держателям счетов. Практический анализ защищенности специализированных банковских систем, который проводят эксперты Positive Technologies, позволяет значительно повысить уровень защиты, предотвратить мошеннические манипуляции с денежными средствами и предотвратить финансовый и репутационный ущерб.

Системы управления технологическими процессами — важнейший элемент бизнес-процесса любого промышленного предприятия. Уникальные по объему и качеству услуги анализа защищенности АСУ ТП и устройств промышленного интернета вещей (IIoT), предоставляемые экспертами Positive Technologies позволят выявить реальные векторы атак на промышленные системы и своевременно выработать комплекс мер по предотвращению последствий — от финансового ущерба до ущерба здоровью и жизни людей и техногенных катастроф.

Анализ защищенности АСУ ТП и Industrial IoT

Тестирование на проникновение

Одним из ключевых методов оценки и повышения качества ИБ компании является тест на проникновение. Он проводится для того, чтобы выявить уязвимые места в элементах ИТ-инфраструктуры, продемонстрировать на практике возможности использования уязвимостей информационных систем и сформировать рекомендации по устранению выявленных недостатков.

Тестирование на проникновение может быть внешним (проводиться для периметра корпоративной сети) и внутренним, когда задача атакующего — получить доступ к конкретной информации или соответствующих привилегий уже внутри корпоративной сети. В зависимости от целей тестирования, оно может проводиться с уведомлением служб и пользователей тестируемой компании или без него (так называемый Red Teaming). В случае применения Wi-Fi в инфраструктуре компании, тестирование на проникновение может быть расширено анализом защищенности беспроводных сетей.

Результаты тестирования на проникновение чаще всего носят сугубо технический характер, но не стоит забывать, что ошибки сотрудников компании — один из наиболее распространенных источников угроз информационной безопасности. Для снижения рисков, связанных с «человеческим фактором» используются различные технические и административные механизмы защиты ИБ. Наряду с исправлениями технических недочетов, выявленных тестированием на проникновение, услуга Positive Technologies по оценке и повышению осведомленности позволяет повысить готовность персонала к кибератаке, в том числе с использованием социотехнических методов, являющихся одними из самых эффективных в арсенале злоумышленников.

Внешнее и внутреннее тестирование на проникновение
Поможет оценить риск и возможности проникновения злоумышленника в сеть компании

Анализ защищенности беспроводных сетей
Поможет повысить безопасность корпоративной Wi-Fi инфраструктуры

Анализ конфигураций сетевого оборудования
Поможет оценить и повысить безопасность настроек устройств сети

Оценка осведомленности пользователей
Поможет повысить готовность персонала к кибератакам

Анализ защищенности приложений

Атаки на веб-приложения — основная причина всех утечек данных и средств из компаний. Это подтверждают и результаты исследования Positive Technologies: в каждом пятом веб-приложении есть уязвимости, позволяющие злоумышленнику получить контроль как над самим приложением, так и над ОС сервера. Если сервер находится на периметре сети организации, злоумышленник может проникнуть во внутреннюю сеть компании — 75% векторов проникновения в ЛВС связаны именно с недостатками защиты веб-приложений. Но не стоит забывать, что веб-приложения активно используются и внутри корпоративных сетей (в том числе для доступа к ERP-системам), и атака на них может являться одним из основных векторов горизонтального развития атаки. И число критически опасных уязвимостей, которое приходится на одно веб-приложение, по сравнению с 2017 годом выросло в 3 раза.

Свести к минимуму риск успешной кибератаки поможет регулярный анализ защищенности веб-приложений. Оценка защищенности веб-приложений может выполняться как с использованием методики «черного ящика», так и путем анализа исходных кодов.

В ходе работ по анализу защищенности веб-приложений используются общепринятые методики анализа и оценки безопасности приложений, в разработке которых эксперты Positive Technologies принимают активное участие: OWASP TOP 10, Web Application Security Consortium Thread Classification и Common Vulnerability Scoring System. Анализу подвергаются все компоненты веб-приложения: дизайн, сетевое взаимодействие, настройки ОС, внешние источники данных, хранилища информации, используемые механизмы авторизации и аутентификации, серверные и клиентские компоненты.

Наряду с веб-приложениями приложения для мобильных устройств стали стандартом де-факто для взаимодействия с клиентами во множестве индустрий — финансовой, торговой, развлекательной. Проблемы с безопасностью приложения могут стать причиной снижения лояльности клиентов и их оттоку. В этих условиях основными целями анализа и повышение защищенности мобильного приложения являются защита пользовательских данных и предотвращение реализации мошеннических схем.

Анализ защищенности веб-приложений
Поможет существенно снизить риск успешной кибератаки как на внешний, так и внутренний периметр компании

Анализ защищенности ERP-систем
Поможет оценить риски ИБ, связанные с критическими системами управления бизнесом

Анализ защищенности мобильных приложении
Поможет повысить защищенность данных ваших клиентов и предотвратить мошенничество

Исследование Positive Technologies: «Уязвимости корпоративных информационных систем, 2019»

О компании

Positive Technologies более 15 лет аккумулирует экспертные знания по практической безопасности и является одним из мировых лидеров в области комплексной защиты крупных информационных систем от современных киберугроз. Компания имеет представительства и R&D-центры не только в России, но и по всему миру, в том числе в Великобритании и Чехии. В нашей команде более 250 экспертов по защите ERP, SCADA, банков и телекомов, веб- и мобильных приложений.

Более 1000 компаний используют решения Positive Technologies для анализа защищенности и соответствия стандартам, а также для мониторинга событий безопасности, блокирования атак, предотвращения вторжений, расследования инцидентов, анализа исходного кода и построения безопасной разработки. Компания трижды становилась «визионером» в исследовании Gartner Magic Quadrant по системам защиты веб-приложений (WAF).

Результаты исследований экспертов Positive Technologies используются для обновления базы знаний системы MaxPatrol, а также для разработки новых продуктов комплексной защиты: PT Application Firewall, PT Application Inspector, MaxPatrol SIEM, PT ISIM, PT MultiScanner и других. Эти решения позволяют обеспечить безопасность веб-приложений, оценить уровень защищенности сетей, блокировать атаки в режиме реального времени, контролировать выполнение нормативных требований и соответствие государственным и корпоративным стандартам, а также обучать специалистов по безопасности.

Репутация экспертов мирового уровня по вопросам защиты самых разнообразных устройств и инфраструктур подтверждена обширным списком наших партнеров и клиентов:

Honeywell Google HUAWEI

Microsoft cisco Schneider Electric

SIEMENS SAP ORACLE

Подробнее:

ptsecurity.ru
facebook.com/PositiveTechnologies
vk.com/ptsecurity
phdays.ru
twitter.com/ptsecurity
ru.ptnews.pro
habr.com/ru/company/pt/

О компании

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.